



# DevSecComp(liance)Ops with OSCAL

March 2022

Ray Gauss, Director of Innovation, Easy Dynamics

# Who is Easy Dynamics?



## Information Sharing

- ✓ B2B and B2C Information Sharing
- ✓ Consent based and full audit traceability
- ✓ Migrations and assessments
- ✓ Digital Identity and governance
- ✓ Knowledge management



## Cloud Delivery

- ✓ Migration readiness, analysis, & planning
- ✓ Enterprise cloud operations
- ✓ Software defined networking
- ✓ DevSecOps and CI/CD as a service
- ✓ FISMA/FedRAMP accreditation



## Cyber/Identity/Privacy

- ✓ Identity and access management
- ✓ Privacy engineering and policy development
- ✓ Compliance framework enforcement
- ✓ Asset, ISVM, Anti-virus, SOC/NOC Integration
- ✓ Risk Management and Fraud Detection

## HISTORY OF INNOVATION



**2020 Public Sector  
Innovation of the Year**



**2018 Public Sector  
Innovation of the Year**



## STANDARDS ALIGNMENT



- ✓ NIST SP800-63 / NIST SP800-53
- ✓ NIST Privacy Framework
- ✓ NIST OSCAL
- ✓ Cybersecurity profile for payroll industry



## ACCREDITATION EXPERIENCE



**DHS**

- ✓ First FISMA High
- ✓ Cloud Factory 2 General Support System (GSS) FISMA High



**Navy**



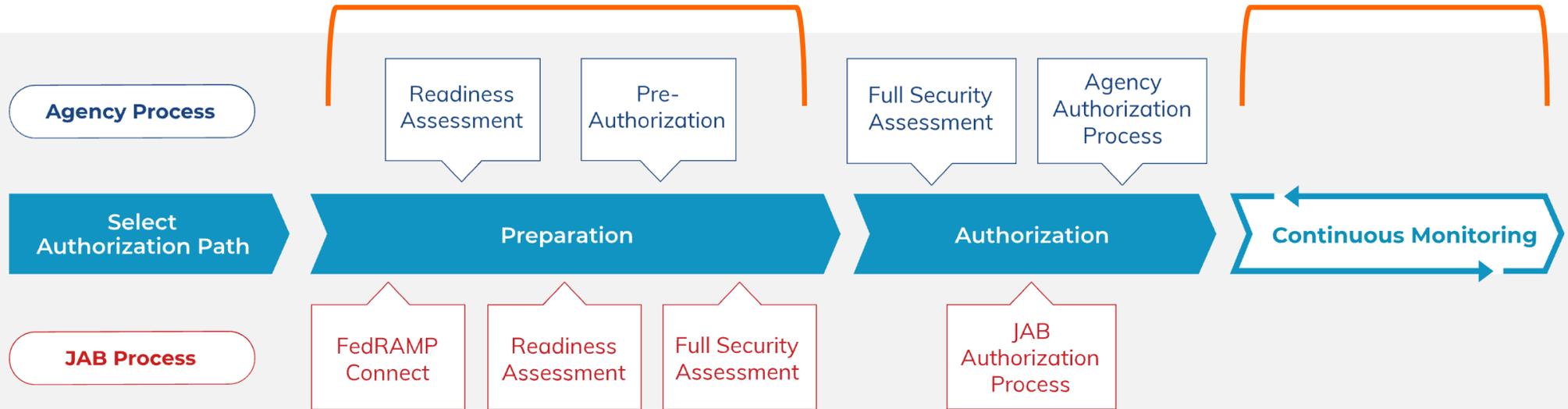
- ✓ FedRAMP Accreditation
- ✓ Early Adopter OSCAL Submission



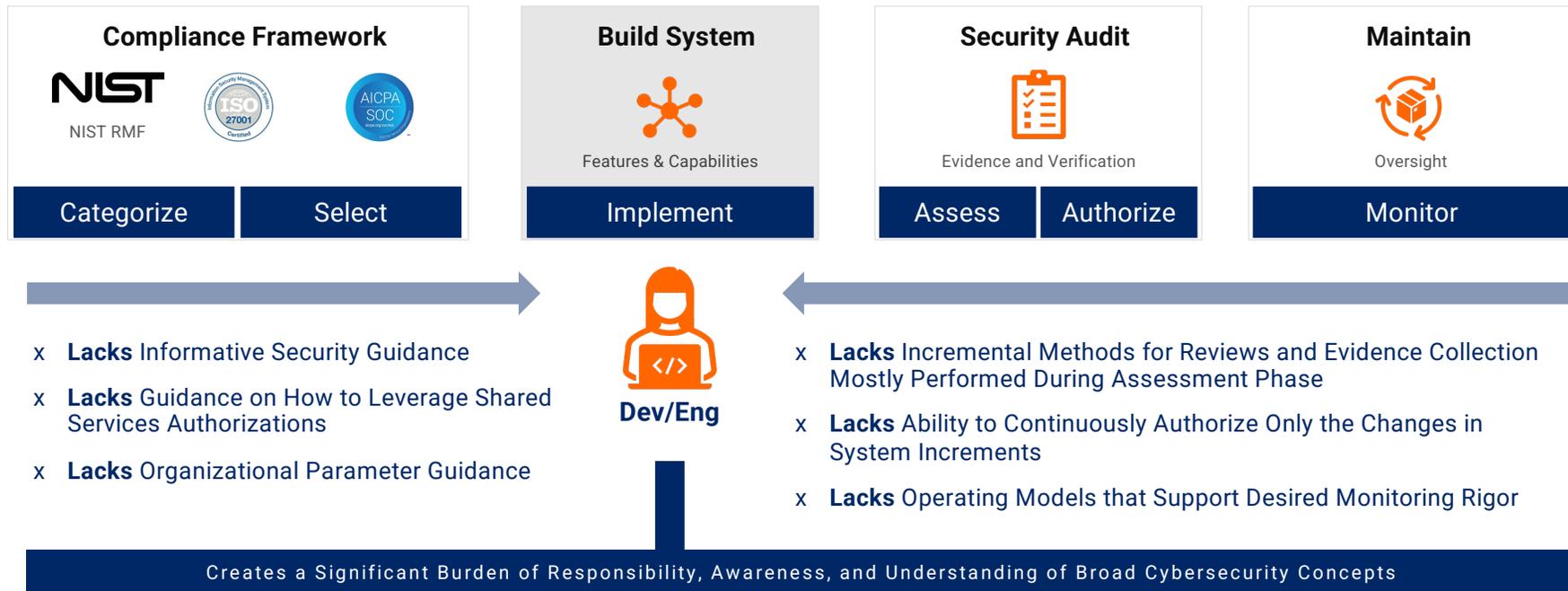
**Education**

# Where We Typically Fit in the Assessment Process

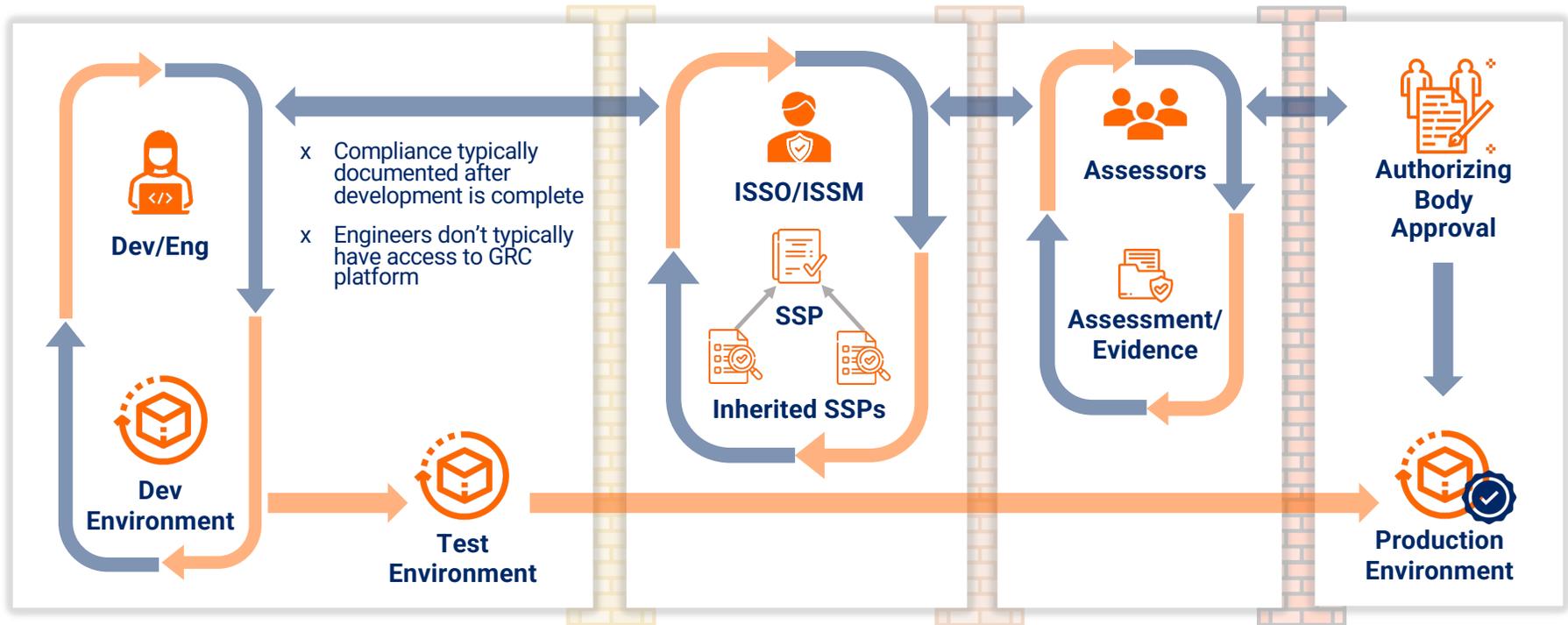
(FedRAMP ATO Example)



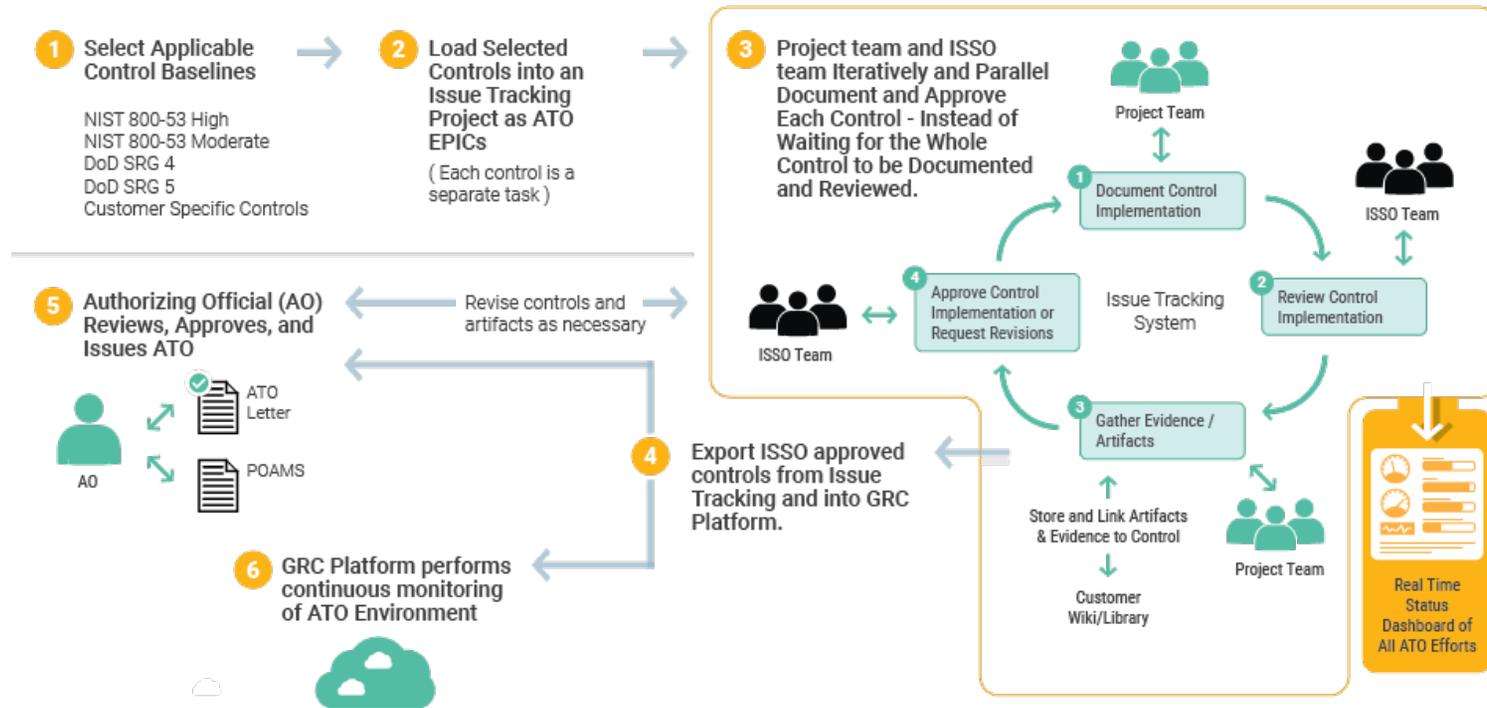
# Challenges We Often See



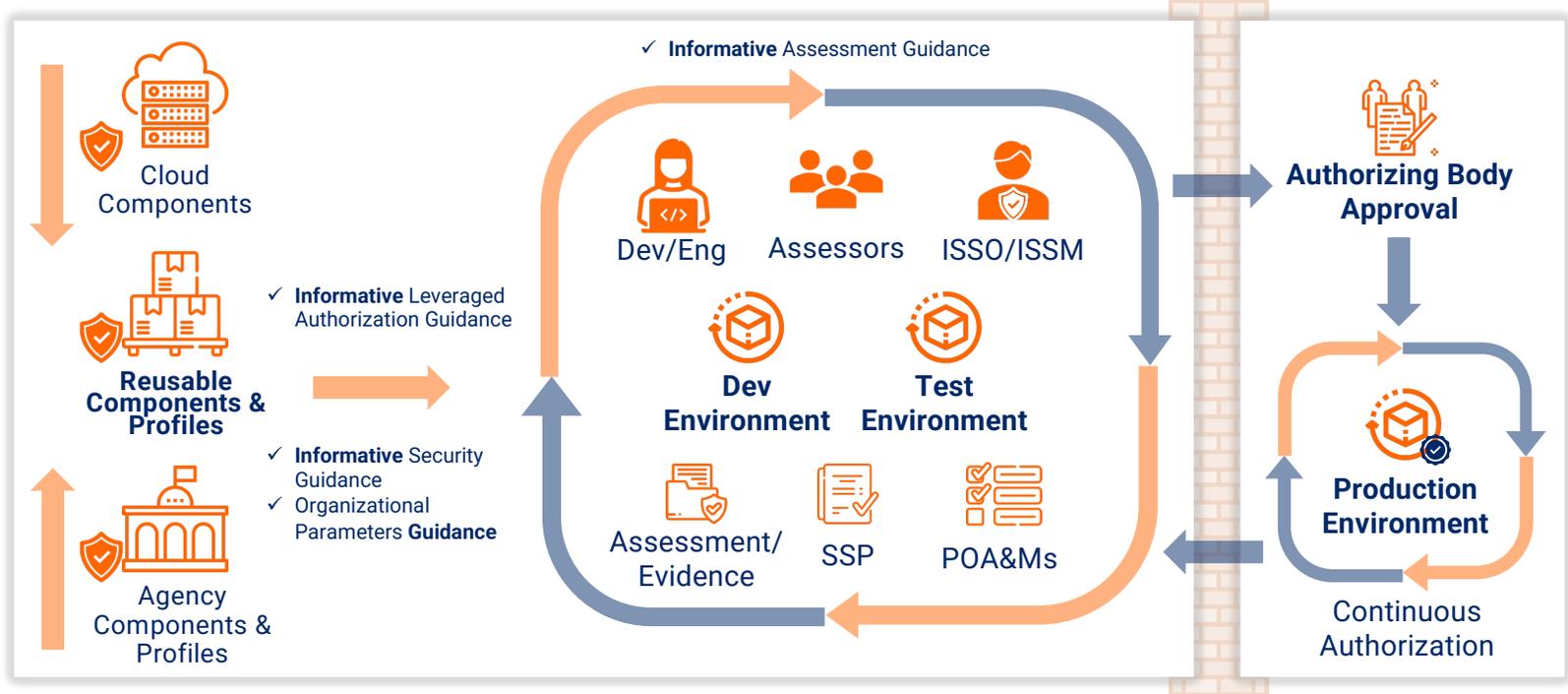
# Traditional Assessment Workflow Has Impediments



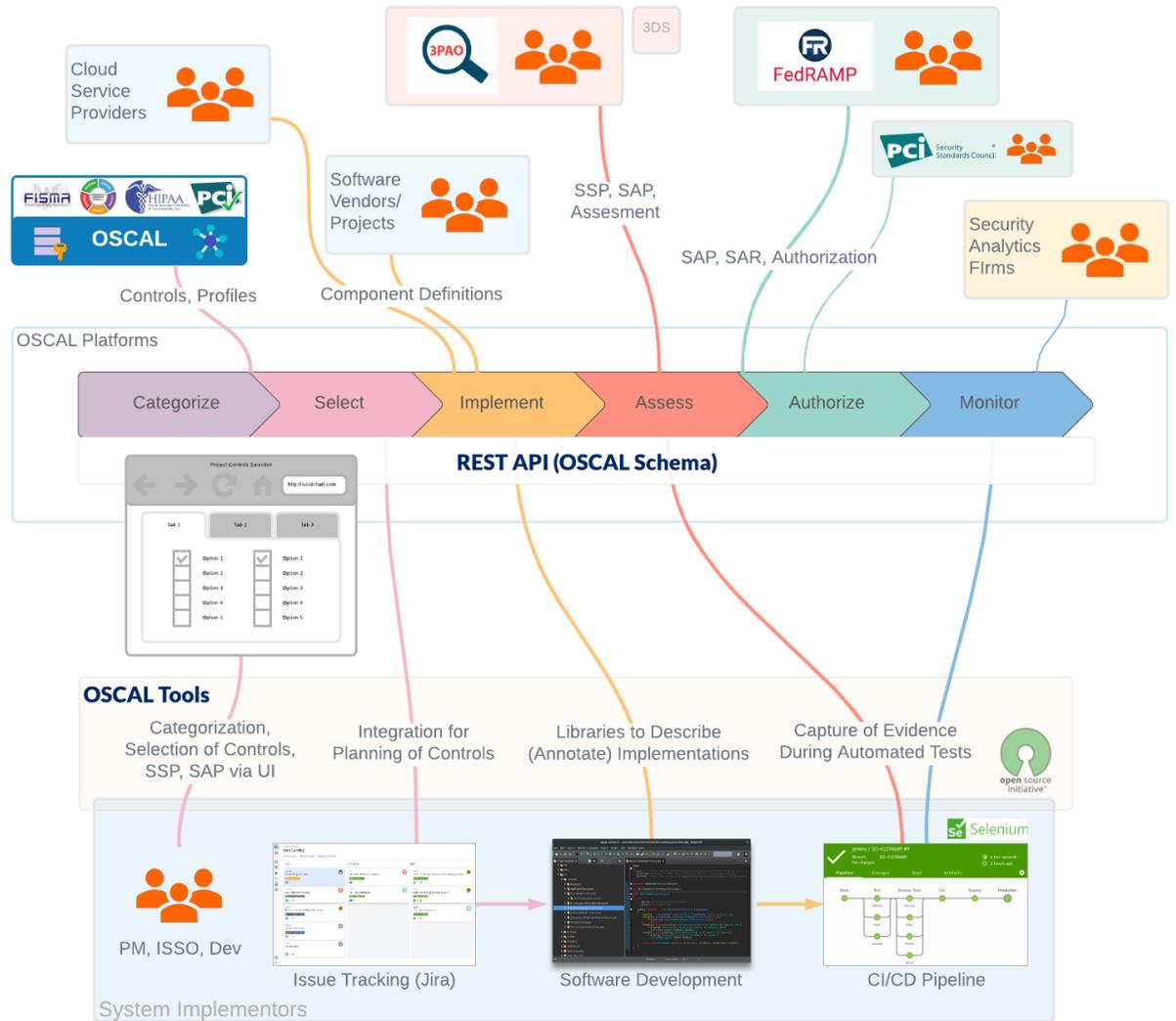
# How We've Addressed These Challenges in the Past



# The Shift-Left Workflow That OSCAL and Tools Enable



# How We See This Space Evolving



# What We've Been Working On

## CONTRIBUTIONS TO DATE

### OSCAL React Component Library and Web App

GitHub Repository <https://github.com/EasyDynamics/oscal-react-library>

Storybook Docs <https://docs.oscal-react-library.msd.easydynamics.com>

Web App Demo <https://oscal-viewer.msd.easydynamics.com>

### OSCAL REST API (OpenAPI)

GitHub Repository <https://github.com/EasyDynamics/oscal-rest>

Swagger Editor <https://editor.swagger.io/?url=...>

## WHAT'S NEW!

### OSCAL REST Service

- ★ Implementation of some of the OSCAL REST API
- ★ Persists against a file store (such as a Git repository)

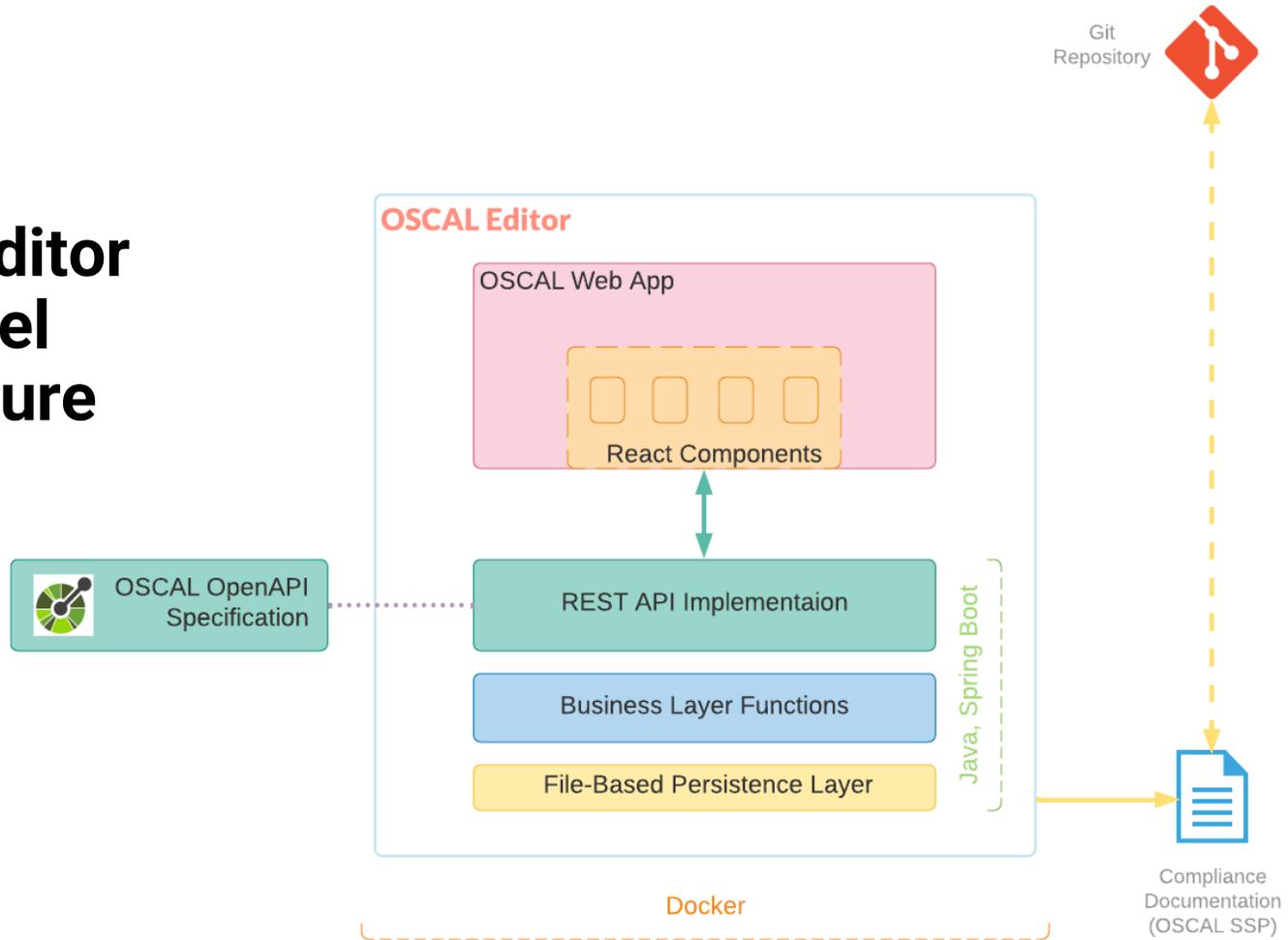
GitHub Repository <https://github.com/EasyDynamics/oscal-rest-service>

### OSCAL Editor

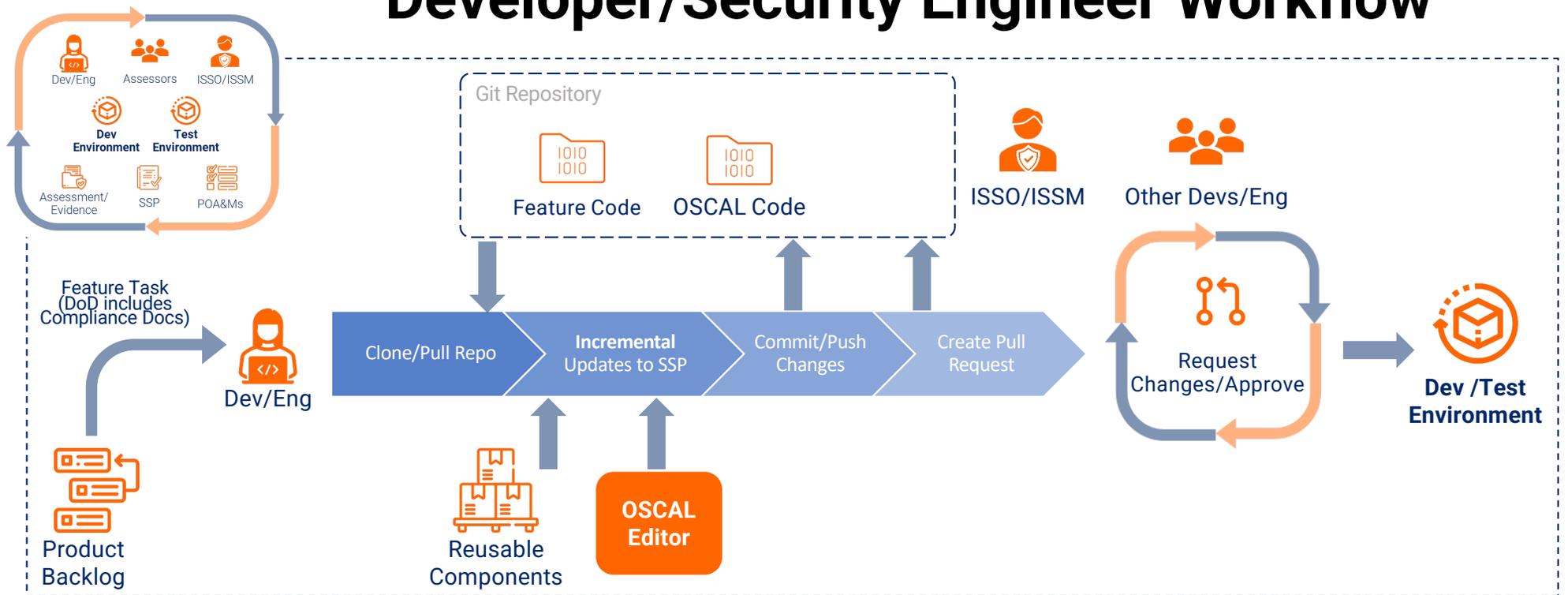
- ★ Docker Container with OSCAL REST Service and Web App

GitHub Repository <https://github.com/EasyDynamics/oscal-editor-deployment>

# OSCAL Editor High-Level Architecture



# Developer/Security Engineer Workflow



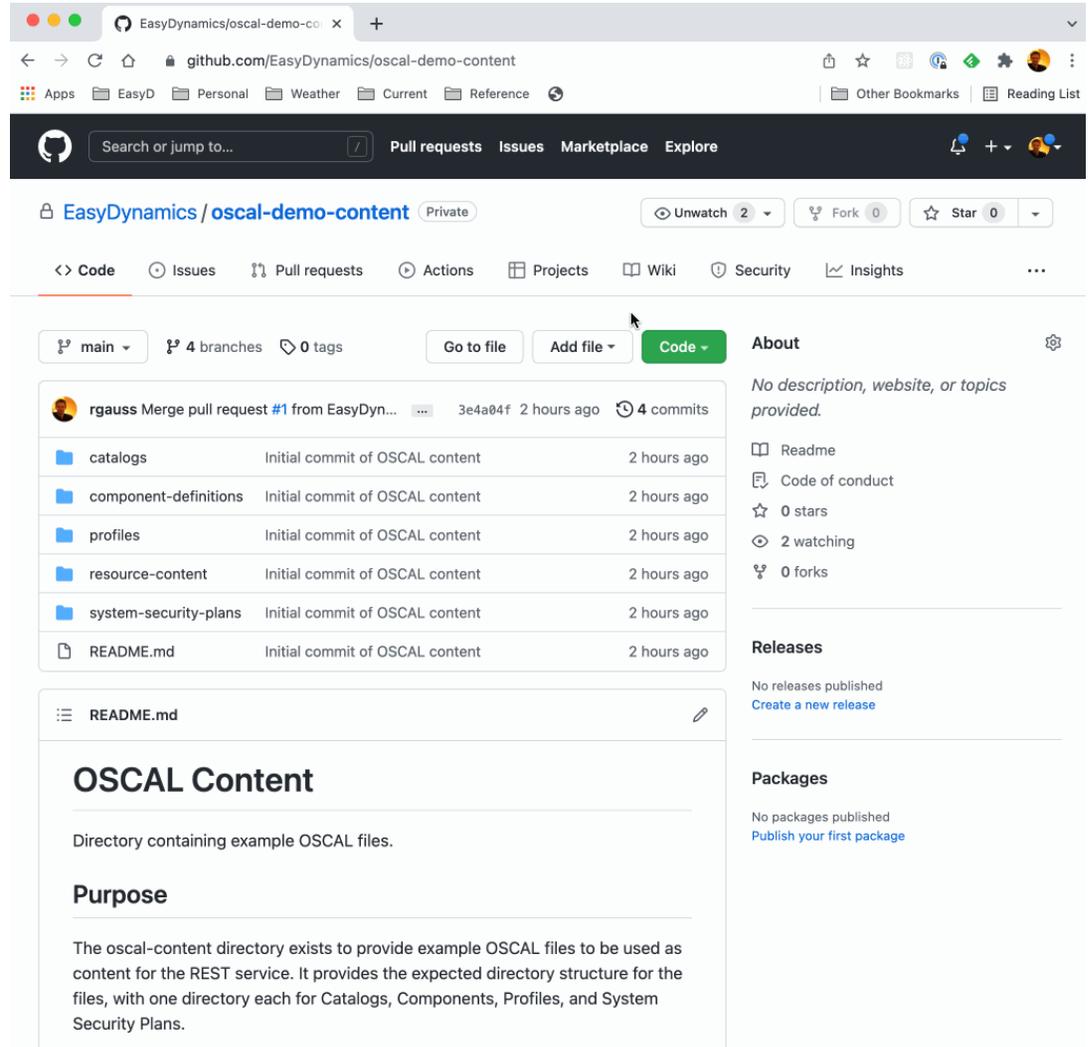


---

# Demo

# Demo

- Dev/Eng
  - Browses OSCAL Content Repository on GitHub
  - Copies Clone URL



The screenshot shows a GitHub repository page for 'EasyDynamics/oscaldemo-content'. The repository is private and has 4 branches, 0 tags, and 4 commits. The repository structure is as follows:

File/Folder	Commit Message	Time
catalogs	Initial commit of OSCAL content	2 hours ago
component-definitions	Initial commit of OSCAL content	2 hours ago
profiles	Initial commit of OSCAL content	2 hours ago
resource-content	Initial commit of OSCAL content	2 hours ago
system-security-plans	Initial commit of OSCAL content	2 hours ago
README.md	Initial commit of OSCAL content	2 hours ago

The README.md file content is as follows:

## OSCAL Content

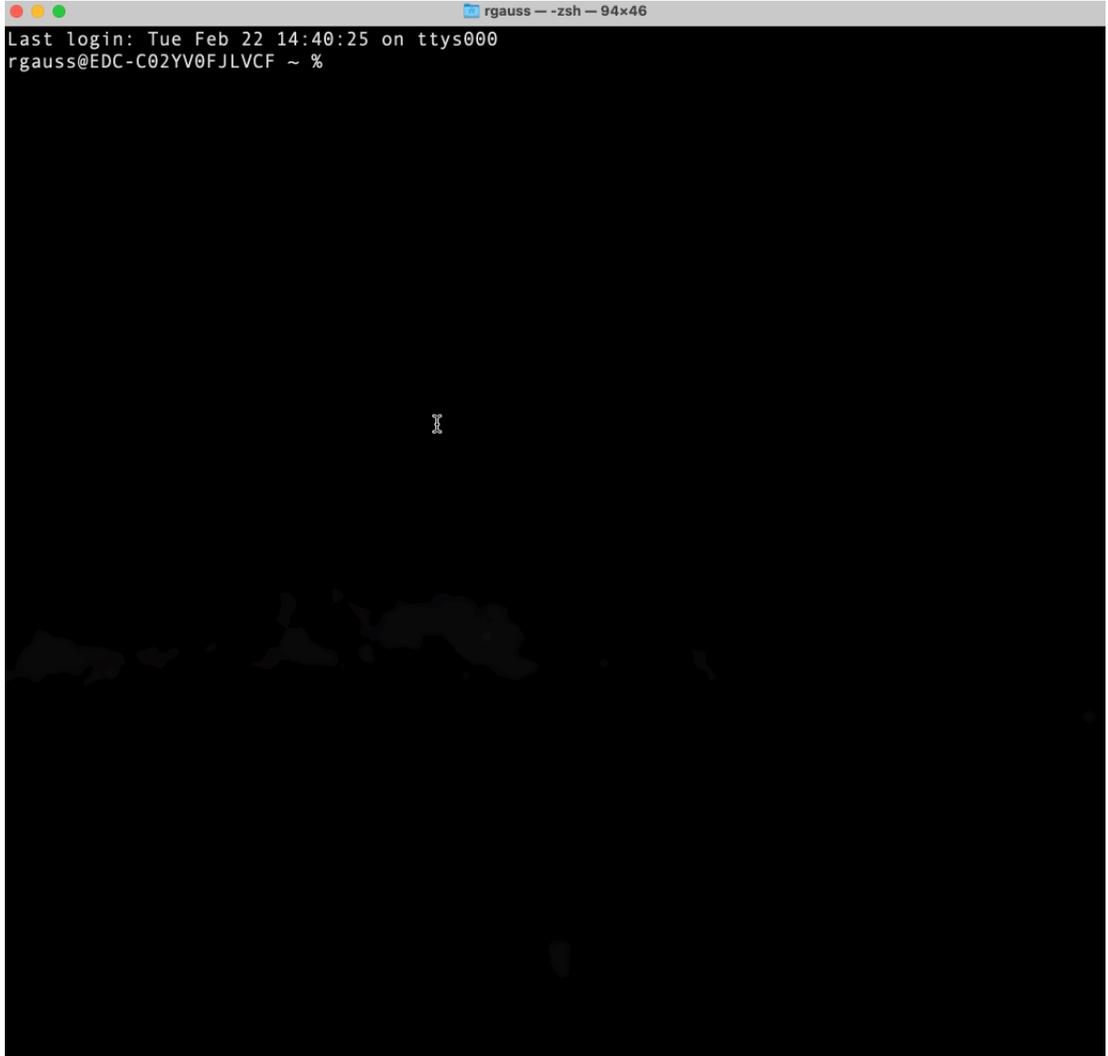
Directory containing example OSCAL files.

### Purpose

The oscal-content directory exists to provide example OSCAL files to be used as content for the REST service. It provides the expected directory structure for the files, with one directory each for Catalogs, Components, Profiles, and System Security Plans.

## Demo

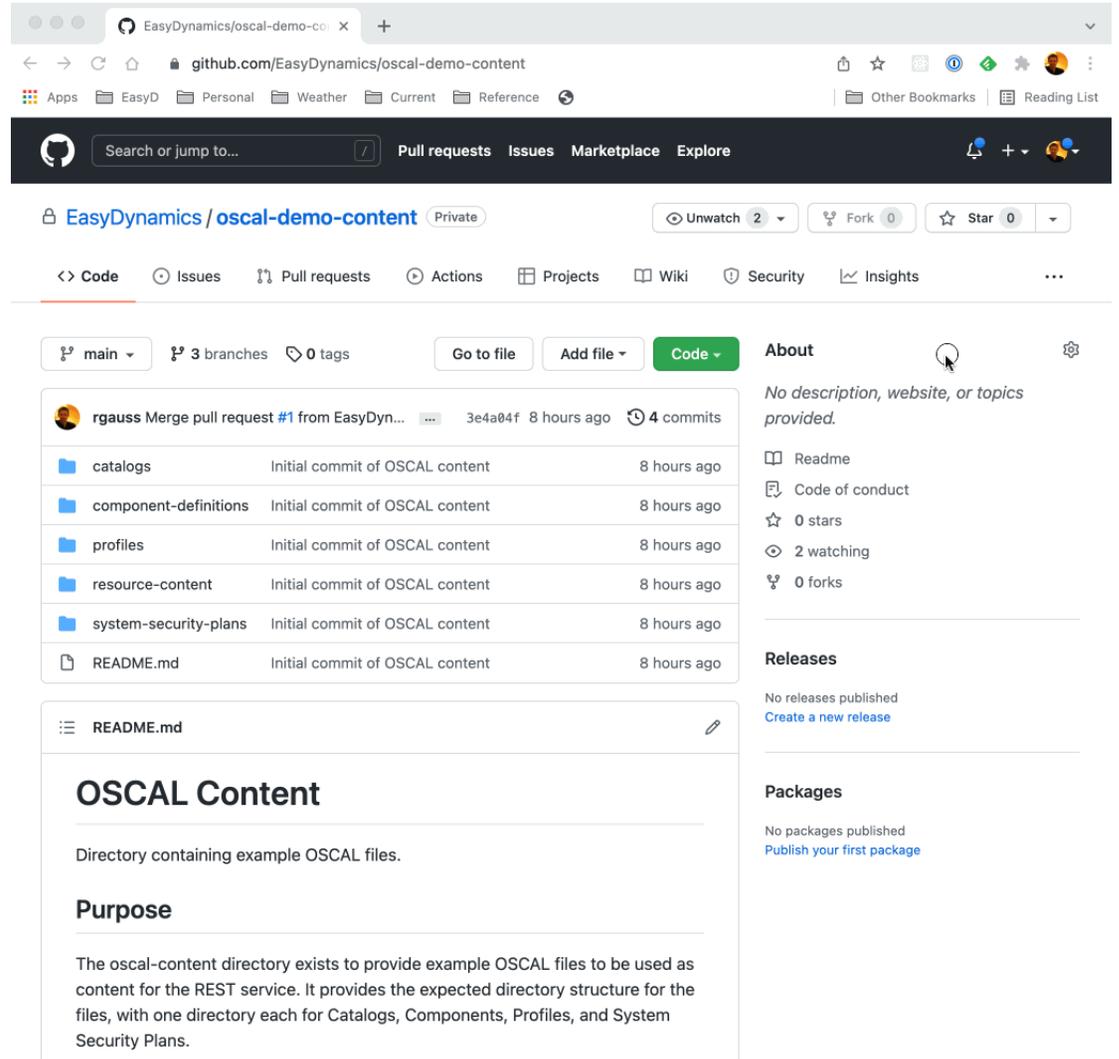
- Dev/Eng
  - Clones OSCAL Content GitHub Repo
  - Pulls Docker Container
  - Runs Docker Container Pointing to Local Content Repo



```
rgauss -- zsh -- 94x46
Last login: Tue Feb 22 14:40:25 on ttys000
rgauss@EDC-C02YV0FJLVCF ~ %
```

# Demo

- Dev/Eng
  - Uses OSCAL Editor to Update SSP Title



EasyDynamics / oscaldemo-content (Private)

Unwatch 2 Fork 0 Star 0

Code Issues Pull requests Actions Projects Wiki Security Insights

main 3 branches 0 tags Go to file Add file Code

rgauss Merge pull request #1 from EasyDyn... 3e4a04f 8 hours ago 4 commits

catalogs	Initial commit of OSCAL content	8 hours ago
component-definitions	Initial commit of OSCAL content	8 hours ago
profiles	Initial commit of OSCAL content	8 hours ago
resource-content	Initial commit of OSCAL content	8 hours ago
system-security-plans	Initial commit of OSCAL content	8 hours ago
README.md	Initial commit of OSCAL content	8 hours ago

README.md

## OSCAL Content

Directory containing example OSCAL files.

### Purpose

The oscal-content directory exists to provide example OSCAL files to be used as content for the REST service. It provides the expected directory structure for the files, with one directory each for Catalogs, Components, Profiles, and System Security Plans.

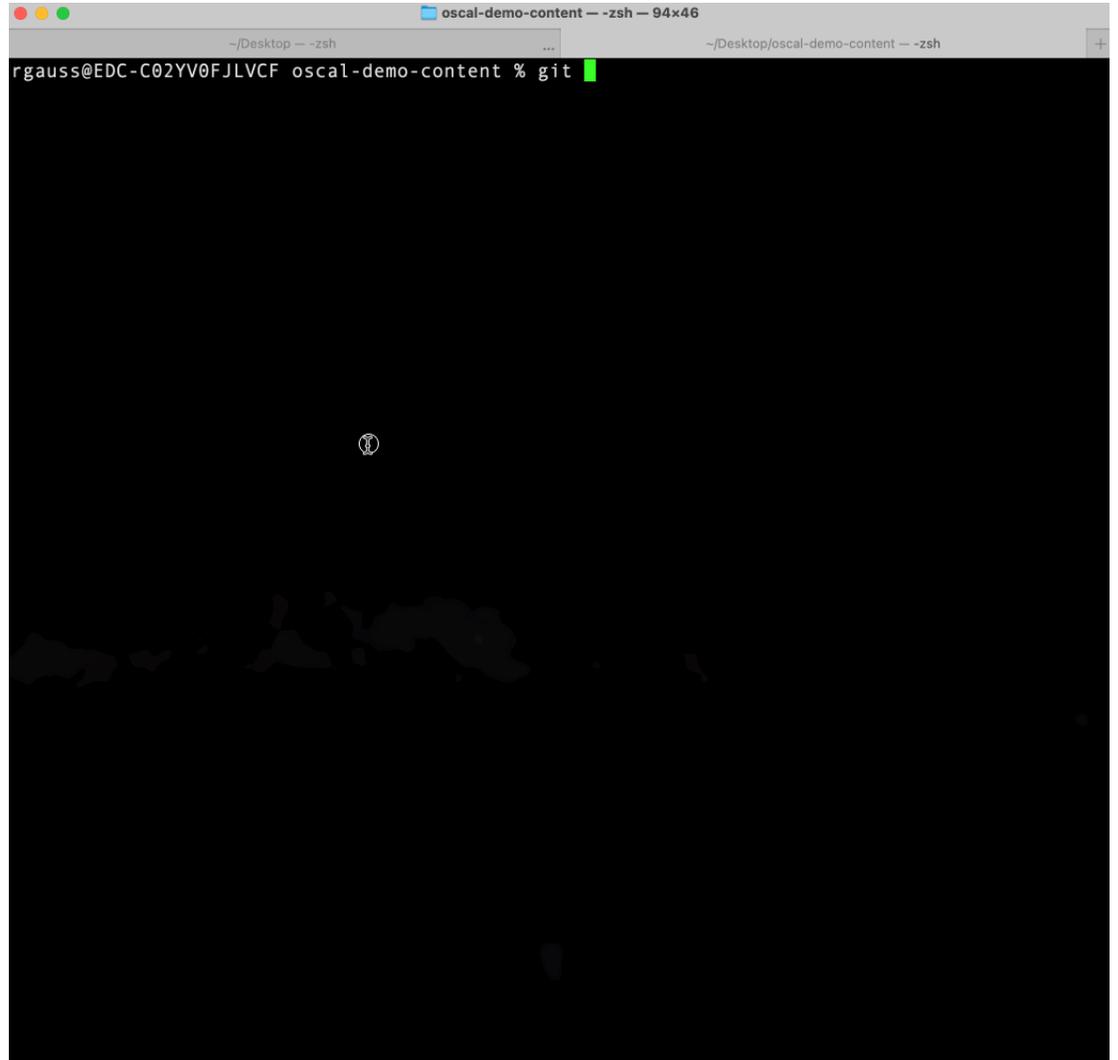
About: No description, website, or topics provided.

Releases: No releases published. [Create a new release](#)

Packages: No packages published. [Publish your first package](#)

## Demo

- Dev/Eng
  - Creates Git Branch
  - Commits Change
  - Pushes New Branch

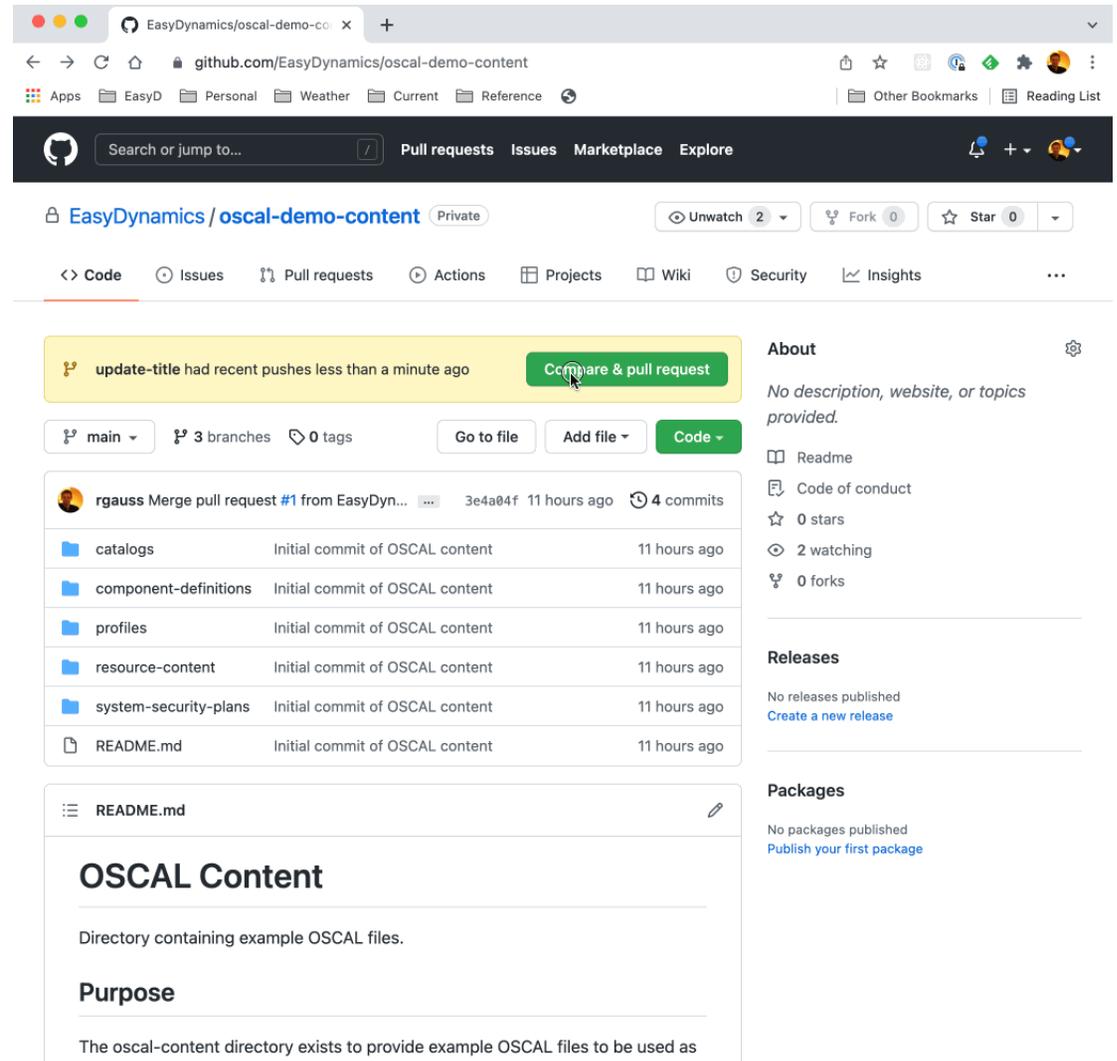


```
rgauss@EDC-C02YV0FJLVCF oscal-demo-content % git
```

The image shows a terminal window with a dark background. The prompt is 'rgauss@EDC-C02YV0FJLVCF oscal-demo-content % git'. The terminal is mostly empty, with a small cursor at the end of the command. The window title bar shows 'oscal-demo-content - zsh - 94x46'.

# Demo

- Dev/Eng
  - Creates PR on GitHub



The screenshot shows a GitHub repository page for `EasyDynamics/oscaldemo-content`. The repository is private and has 2 unwatchers, 0 forks, and 0 stars. The main branch is selected, and there are 3 branches and 0 tags. A recent commit by `rgauss` is shown, titled "Merge pull request #1 from EasyDyn...", with a commit hash of `3e4a04f` and 4 commits. The commit message is "update-title had recent pushes less than a minute ago". A green button labeled "Compare & pull request" is visible next to the commit. Below the commit, a list of files is shown, including `catalogs`, `component-definitions`, `profiles`, `resource-content`, `system-security-plans`, and `README.md`. The `README.md` file is selected, and its content is displayed below. The README content includes the title "OSCAL Content", a description "Directory containing example OSCAL files.", and a section titled "Purpose" with the text "The oscal-content directory exists to provide example OSCAL files to be used as".

**About**

No description, website, or topics provided.

**Releases**

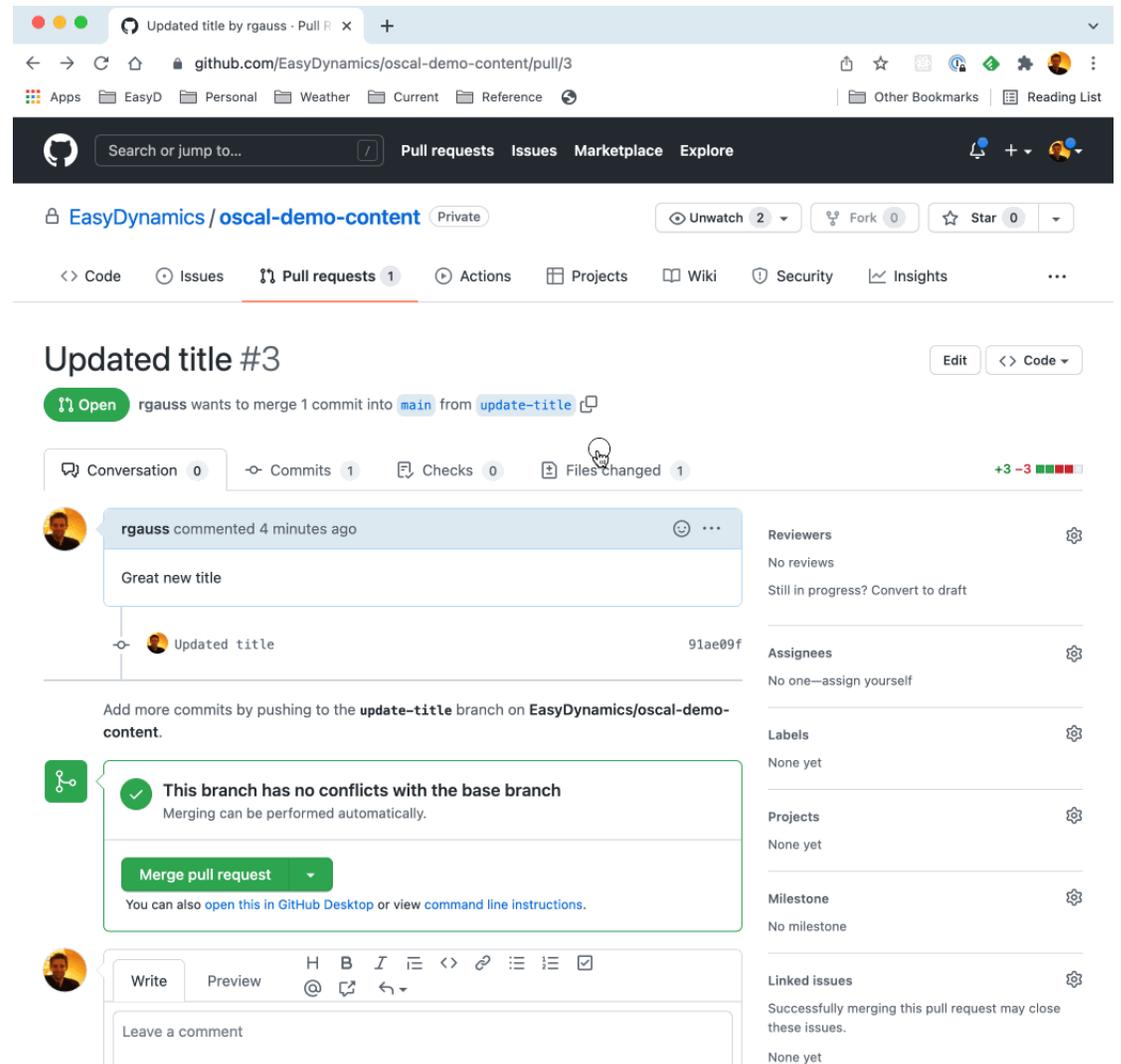
No releases published  
[Create a new release](#)

**Packages**

No packages published  
[Publish your first package](#)

# Demo

- ISSO/ISSM
  - Review PR on GitHub



The screenshot shows a GitHub pull request interface. At the top, the browser address bar displays the URL `github.com/EasyDynamics/oscal-demo-content/pull/3`. The repository name is `EasyDynamics / oscal-demo-content`. The pull request title is `Updated title #3`. The pull request is from the `update-title` branch to the `main` branch. A comment from `rgauss` says "Great new title". A green box indicates that the branch has no conflicts with the base branch and that merging can be performed automatically. A "Merge pull request" button is visible. The right sidebar shows the "Reviewers" section with "No reviews" and "Still in progress? Convert to draft". The "Assignees" section shows "No one—assign yourself". The "Labels" section shows "None yet". The "Projects" section shows "None yet". The "Milestone" section shows "No milestone". The "Linked issues" section shows "Successfully merging this pull request may close these issues." and "None yet".

## What's Next?

- REST API Improvements
  - With the OSCAL Community's Help
- React Component Library & Web App Improvements
  - Expanded Edit Capabilities
  - UI/UX Improvements
- OSCAL Standards
  - Registry Specification
    - Component Definitions In Particular
- CI/CD Integration
  - Validation
  - Attachment of Evidence
- IDE Extensions

## Questions / More Info

- <https://easydynamics.com/oscal>
- <https://github.com/EasyDynamics>
  - [oscal-react-library](#)
  - [oscal-rest](#)
  - [oscal-rest-service](#)
  - [oscal-editor-deployment](#)